PENDING CLAIMS AS AMENDED

Please amend the claims as follows:

1. (Currently Amended) A method of generating a key stream comprising:

selecting ~~applying a cryptographic function on at least five~~ input words ~~values selected~~ from a first array of words, wherein each input word comprises two or more bytes ~~values to generate at least five output values~~;

mixing at least two input words to generate primary mixed words;

performing a byte-wise substitution of at least one byte of each of the primary mixed words to generate respective primary intermediate words;

mixing at least two bytes of each of the primary intermediate words to generate respective secondary intermediate words;

mixing at least two secondary intermediate words to generate output words;

selecting ~~at least five~~ mask words ~~values~~ from a second array of words ~~values~~; and

combining the ~~at least five~~ output words ~~values~~ with the ~~at least five~~ mask words ~~values~~ to generate a key stream block for the key stream;

wherein the first and second arrays are finite.

2. (Original) The method of claim 1, further comprising: generating the second array from the first array.

3. (Currently Amended) The method of claim 2, further comprising: using a linear feedback shift register (LFSR) to generate the first array, wherein the words ~~values~~ of the first array correspond to ~~the values of the~~ LFSR states.

4. (Original) The method of claim 3, further comprising: clocking the LFSR to generate the second array.

5. (Currently Amended) The method of claim 3, wherein ~~each value comprises of one or more words, each of two or more bytes and wherein~~ using the LFSR to generate the first array comprises:

copying words of a key and words of an initialization vector into the LFSR;

performing a byte-wise substitution on at least one byte of a word in the LFSR to generate a corresponding replacement word in the LFSR;

mixing at least two bytes of a replacement word in the LFSR; and

mixing at least two words in the LFSR to generate the first array.

6. (Currently Amended) The method of claim 1, further comprising:

selecting ~~applying the cryptographic function on~~ updated input words ~~values selected~~ from an updated first array of words for generating ~~values to generate~~ updated output words ~~values~~;

selecting updated mask words ~~values~~ from an updated second array of words ~~values~~; and

combining the updated output words ~~values~~ with the updated mask words ~~values~~ to generate a new key stream block for the key stream.

7. (Currently Amended) The method of claim 6, further comprising: setting the words ~~values~~ of the first array based on ~~as the values of~~ first linear feedback shift register (LFSR) states; and clocking the LFSR to generate the updated first array.

8. (Currently Amended) The method of claim 6, further comprising: setting the words ~~values~~ of the second array based on ~~as the values of~~ second LFSR states; and clocking the LFSR to generate the updated second array.

9. (Currently Amended) The method of claim 1, wherein the number of input words ~~values~~ and the number of output words ~~values~~ are each equal to five.

10. (Currently Amended) The method of claim 1, wherein the first and second array each comprises seventeen words ~~values~~.

11-12. (Canceled).

13. (Currently Amended) The method of claim 1 [[12]], wherein performing the byte-wise substitution of at least one byte comprises: performing a nonlinear substitution of the at least one byte.

14. (Original) The method of claim 13, wherein performing the nonlinear substitution of the at least one byte comprises: performing a key-dependent Sbox substitution on the at least one byte.

15. (Original) The method of claim 14, wherein performing the key-dependent Sbox substitution of the at least one byte comprises:

combining a first key byte with the at least one byte to generate a first combined byte; and

substituting the first combined byte with a byte value from a pre-determined array.

16. (Original) The method of claim 15, further comprising: generating the first key byte based on a secret key of one or more words.

17. (Original) The method of claim 16, wherein generating the first key comprises:

performing a byte-wise substitution of at least one byte of a word of the secret key to generate a corresponding replacement word; and

mixing at least two bytes of a replacement word to generate the first key byte.

18. (Original) The method of claim 15, wherein performing the key dependent Sbox substitution further comprises:

combining a second key byte with the substituted first combined byte to generate a second combined byte; and

substituting the second combined byte with a byte value from the predetermined array.

19. (Currently Amended) The method of claim 1 [[12]], wherein mixing at least two bytes of each of the primary intermediate words ~~values~~ comprises: mixing at least two bytes using a minimum distance separable matrix multiplication.

20. (Original) The method of claim 19, wherein the minimum distance separable matrix multiplication comprises operations over a Galois Field comprising 256 elements.

21. (Canceled).

22. (Currently Amended) The method of claim 1 [[21]], wherein mixing at least two input words ~~values~~ comprises: mixing the at least two input words ~~values~~ based on modular arithmetic.

23. (Currently Amended) The method of claim 22, wherein mixing at least two input words ~~values~~ comprises:

adding the input words ~~values~~ to generate a first primary mixed word ~~value, wherein the mixed value is a primary intermediate value~~ corresponding to a first input word ~~value~~; and

adding the first primary mixed word ~~value~~ with a second input word ~~value~~ to generate a second primary mixed word ~~intermediate value~~ corresponding to the second input word ~~value~~.

24. (Canceled).

25. (Currently Amended) The method of claim 1 [[24]], wherein mixing at least two secondary intermediate words ~~values~~ comprises: mixing at least two ~~input~~ secondary intermediate words ~~values~~ based on modular arithmetic.

26. (Currently Amended) The method of claim 25, wherein mixing at least two secondary intermediate words ~~values~~ comprises:

adding the secondary intermediate words ~~values~~ to generate a first secondary mixed word ~~value~~, wherein the first secondary mixed word ~~value~~ is an output word ~~value~~ corresponding to a first secondary intermediate word ~~value~~; and

adding the secondary mixed word ~~value~~ with a second secondary intermediate word ~~value~~ to generate an output word ~~value~~ corresponding to the second secondary intermediate word ~~value~~.

27. (Currently Amended) Apparatus for generating a key stream comprising:

means for selecting ~~applying a cryptographic function on at least five~~ input words ~~values selected~~ from a first array of words, wherein each input word comprises two or more bytes ~~values to generate at least five output values~~;

means for mixing at least two input words to generate primary mixed words;

means for performing a byte-wise substitution of at least one byte of each of the primary mixed words to generate respective primary intermediate words;

means for mixing at least two bytes of each of the primary intermediate words to generate respective secondary intermediate words;

mixing at least two secondary intermediate words to generate output words;

means for selecting ~~at least five~~ mask words ~~values~~ from a second array of words ~~values~~; and

means for combining the ~~at least five~~ output words ~~values~~ with the ~~at least five~~ mask words ~~values~~ to generate a key stream block for the key stream; wherein the first and second arrays are finite.

28. (Original) The apparatus of claim 27, further comprising: means for generating the second array from the first array.

29. (Currently Amended) The apparatus of claim 27, further comprising:

means for selecting ~~applying the cryptographic function on~~ updated input words ~~values selected~~ from an updated first array of words for generating ~~values to generate~~ updated output words ~~values~~;

means for selecting updated mask words ~~values~~ from an updated second array of words ~~values~~; and

means for combining the updated output words ~~values~~ with the updated mask words ~~values~~ to generate a new key stream block for the key stream.

30. (Currently Amended) The apparatus of claim 27, wherein the number of input words ~~values~~ and the number of output words ~~values~~ are each equal to five.

31-32. (Canceled).

33. (Currently Amended) The apparatus of claim 27 [[32]], wherein the means for performing byte-wise substitution comprises: means for performing a key-dependent Sbox substitution on the at least one byte.

34. (Currently Amended) The apparatus of claim 27 [[32]], wherein the means for mixing at least two bytes of each of the primary intermediate words ~~values~~ comprises: means for mixing at least two bytes using a minimum distance separable matrix multiplication.

35. (Currently Amended) The apparatus of claim 27 [[32]], wherein the ~~means for applying the cryptographic function further comprises:~~ means for mixing at least two input words is ~~values~~ based on modular arithmetic to generate the primary mixed words ~~intermediate values~~.

36. (Currently Amended) The apparatus of claim 27 [[32]], wherein the ~~means for applying the cryptographic function further comprises:~~

means for mixing at least two secondary intermediate words is ~~values~~ based on modular arithmetic to generate the output words ~~values~~.

37. (Currently Amended) A machine readable medium having one or more instructions for generating a key stream, which when executed by a machine, causes the machine to perform operations comprising:

selecting ~~applying a cryptographic function on at least five~~ input words ~~values selected~~ from a first array of words, wherein each input word comprises two or more bytes ~~values to generate at least five output values~~;

mixing at least two input words to generate primary mixed words;

performing a byte-wise substitution of at least one byte of each of the primary mixed words to generate respective primary intermediate words;

mixing at least two bytes of each of the primary intermediate words to generate respective secondary intermediate words;

mixing at least two secondary intermediate words to generate output words;

selecting ~~at least five~~ mask words ~~values~~ from a second array of words ~~values~~; and

combining the ~~at least five~~ output words ~~values~~ with the ~~at least five~~ mask words ~~values~~ to generate a key stream block for the key stream;

wherein the first and second arrays are finite.

38. (Previously Presented) The medium of claim 37, further comprising one or more instructions to cause the machine to perform operations comprising: generating the second array from the first array.

39. (Canceled).

40. (Currently Amended) The medium of claim 37 [[39]], wherein performing the byte-wise substitution comprises: comprises one or more instructions to cause the machine to perform operations comprising: performing a key-dependent Sbox substitution on the at least one byte.

41. (Currently Amended) The medium of claim 37 [[39]], wherein mixing at least two bytes of each of the primary intermediate words ~~values~~ comprises one or more instructions to cause the machine to perform operations comprising: mixing at least two bytes using a minimum distance separable matrix multiplication.

42. (Currently Amended) The medium of claim 37 [[41]], wherein ~~applying the cryptographic function further comprises one or more instructions to cause the machine to perform operations comprising:~~ mixing at least two input words is ~~values~~ based on modular arithmetic to generate the primary mixed words ~~intermediate values~~.

43. (Currently Amended) The medium of claim 37 [[41]], wherein ~~applying the cryptographic function further comprises one or more instructions to cause the machine to perform operations comprising:~~ mixing at least two secondary intermediate words is ~~values~~ based on modular arithmetic to generate the output words ~~values~~.

44. (Currently Amended) Apparatus for generating a key stream comprising:

a linear feedback shift register (LFSR) configured to generate a first array of words ~~values~~, wherein the words ~~values~~ of the first array corresponds to the values of the LFSR states;

a nonlinear filter module configured to select ~~apply a cryptographic function on at least five~~ input words ~~values selected~~ from the first array of words, wherein each input word comprises two or more bytes ~~to generate at least five output values~~;

a first word mixing module configured to mix at least two input words to generate primary mixed words;

a byte substitution module configured to perform byte-wise substitution of at least one byte of each of the primary mixed words to generate respective primary intermediate words;

a byte mixing module configured to mix at least two bytes of each of the primary intermediate words to generate respective secondary intermediate words;

a second word mixing module configured to mix at least two secondary intermediate words to generate output words; and

a combining module configured to combine the ~~at least five~~ output words ~~values~~ with ~~at least five~~ mask words ~~values~~ selected from a second array of words ~~values~~ to generate a key stream block for the key stream; wherein the first and second arrays are finite.

45. (Original) The apparatus of claim 44, wherein the LFSR is configured to generate the second array from the first array.

46. (Currently Amended) The apparatus of claim 44, wherein the number of input words ~~values~~ and the number of output words ~~values~~ are each equal to five.

47. (Currently Amended) The apparatus of claim 44, wherein the first and second array each comprises seventeen words ~~values~~.

48-49. (Canceled).

50. (Currently Amended) The apparatus of claim 44 [[49]], wherein the byte substitution module is configured to perform a key-dependent Sbox substitution on the at least one byte.

51. (Currently Amended) The apparatus of claim 44 [[49]], wherein the byte mixing module is configured to mix at least two bytes using a minimum distance separable matrix multiplication.

52. (Currently Amended) The apparatus of claim 44 [[49]], wherein the ~~nonlinear filter further comprises: a~~ first word mixing module is further configured to mix at least two input words ~~values~~ based on modular arithmetic to generate the primary mixed words ~~intermediate values~~.

53. (Currently Amended) The apparatus of claim 44 [[49]], wherein ~~the nonlinear filter further comprises: a~~ second word mixing module is further configured to mix at least two secondary intermediate words ~~values~~ based on modular arithmetic to generate the output words ~~values~~.

54. (Currently Amended) The apparatus of claim 44, wherein

each ~~input value,~~ output word ~~value,~~ and mask ~~value comprises one or more words, each~~ word has ~~having~~ two or more bytes, and

the key stream block comprises five or more words, each word having two or more bytes.

55. (Currently Amended) The method of claim 1, wherein

each ~~input value,~~ output word ~~value,~~ and mask ~~value comprises one or more words, each~~ word has ~~having~~ two or more bytes, and

the key stream block comprises five or more words, each word having two or more bytes.

56. (Currently Amended) The apparatus of claim 27, wherein

each ~~input value,~~ output word ~~value,~~ and mask ~~value comprises one or more words, each~~ word has ~~having~~ two or more bytes, and

the key stream block comprises five or more words, each word having two or more bytes.

57. (Currently Amended) The medium of claim 37, wherein

each ~~input value,~~ output word ~~value,~~ and mask ~~value comprises one or more words, each~~ word has ~~having~~ two or more bytes, and

the key stream block comprises five or more words, each word having two or more bytes.